Office of the Information and
Privacy Commissioner of Alberta

PERSONAL INFORMATION PROTECTION ACT
Breach Notification Decision

Organization providing notice under section 34.1 of PIPA	SMART Local Unions and Councils Pension Fund (Canada) (Organization)
Decision number (file number)	P2021-ND-097 (File #013385)
Date notice received by OIPC	June 11, 2019
Date Organization last provided information	June 11, 2019
Date of decision	March 31, 2021
Summary of decision	There is a real risk of significant harm to the individuals affected by this incident. The Organization is required to notify the individuals whose personal information was collected in Alberta, pursuant to section 37.1 of the *Personal Information Protection Act* (PIPA).
JURISDICTION	
Section 1(1)(i) of PIPA "organization"	The Organization is an "organization" as defined in section 1(1)(i) of PIPA.
Section 1(1)(k) of PIPA "personal information"	The incident may have involved the following information: • name, • employer name, • email address, • salary, • date of birth, and • social insurance number. This information is about identifiable individuals and is "personal information" as defined in section 1(1)(k) of PIPA. To the extent the information was collected in Alberta, PIPA applies.
DESCRIPTION OF INCIDENT	
❑ loss ☒ unauthorized access ❑ unauthorized disclosure	
Description of incident	• As a result of a successful phishing attack, an intruder was able to obtain the credentials for an email account assigned to an employee of a service provider to the Organization and gain access to certain emails.

	• The incident occurred on May 20, 2019 and was discovered on May 28, 2019 when the employee who was the subject of the successful email phishing attempt reported the incident.
Affected individuals	The incident affected 3 individuals in Alberta.
Steps taken to reduce risk of harm to individuals	• Arranged for credit monitoring and identity theft insurance for 2 years at no cost and offered to reimburse affected individuals for optional fraud alerts. • Advised individuals of steps to take to protect themselves from phishing. • Completed a security review with input from external advisors and implementing additional security controls.
Steps taken to notify individuals of the incident	Affected individuals were notified by mail and telephone on June 10, 2019.
REAL RISK OF SIGNIFICANT HARM ANALYSIS	
Harm Some damage or detriment or injury that could be caused to affected individuals as a result of the incident. The harm must also be "significant." It must be important, meaningful, and with non-trivial consequences or effects.	The Organization reported that "The relevant possible harms include the possibility of identity theft, financial fraud, and increased risk of spear phishing attempts." I agree with the Organization's assessment. A reasonable person would consider that the contact, identity and employment information at issue could be used to cause the harms of identity theft and fraud. Email address could be used for phishing, increasing vulnerability to identity theft and fraud. These are significant harms.
Real Risk The likelihood that the significant harm will result must be more than mere speculation or conjecture. There must be a cause and effect relationship between the incident and the possible harm.	The Organization reported "Previous Notification Decisions of the Commissioner have found similar incidents to constitute a real risk of signifcant [sic] harm to affected individuals." In my view, a reasonable person would consider that the likelihood of harm resulting from this incident is increased because the incident appears to be the result of malicious intent (deliberate, phishing, compromised credentials). The information appears to have been exposed for over 1 week before the compromise was discovered.
DECISION UNDER SECTION 37.1(1) OF PIPA	
Based on the information provided by the Organization and given the circumstances of the incident, I have decided that there is a real risk of significant harm to the affected individuals.	

A reasonable person would consider that the contact, identity and employment information at issue could be used to cause the harms of identity theft and fraud. Email address could be used for phishing, increasing vulnerability to identity theft and fraud. These are significant harms.

The likelihood of harm resulting from this incident is increased because the incident appears to be the result of malicious intent (deliberate, phishing, compromised credentials). The information appears to have been exposed for over 1 week before the compromise was discovered.

I require the Organization to notify the affected individuals whose personal information was collected in Alberta, in accordance with section 19.1 of the *Personal Information Protection Act Regulation* (Regulation).

I understand the affected individuals were notified by mail and telephone on June 10, 2019. The Organization is not required to notify the affected individuals again.

Jill Clayton
Information and Privacy Commissioner